

Appl. No. 09/885,959

Amdt. Dated: May 19, 2005

Reply to Office Action of: November 19, 2004

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method for multiplying an elliptic curve point $Q(x,y)$ by a scalar k to provide a point kQ , the method comprising the steps of:
 - a) selecting an elliptic curve of order n over a finite field F such that there exists an endomorphism ψ where $\psi(Q) = \lambda(Q)$ for all point $Q(x,y)$ on the elliptic curve, and λ is an integer[[,]] ;
 - b) establishing a representation of said scalar k as a combination of components k_i and said integer λ of the form $k_i = \sum_{i=0}^{l-1} k_i \lambda^i \bmod n[[,]]$;
 - c) combining said representation and said point Q to form a composite representation of a multiple of the form $k_0 Q + k_1 \psi(Q) + \dots + k_{l-1} \psi^{l-1}(Q) + \dots$ corresponding to kQ ; and
 - d) computing a value corresponding to said point kQ from said composite representation of kQ .
2. (original) A method according to claim 1 wherein each of said components k_i is shorter than said scalar k .
3. (original) A method according to claim 1 wherein said components k_i are initially selected and subsequently combined to provide said scalar k .
4. (previously presented) A method according to claim 1 wherein said components k_i are selected at random.
5. (previously presented) A method according to claim 4 wherein said representation is of the form $k_0 + k_1 \lambda$.
6. (previously presented) A method according to claim 1 wherein said scalar k has a

Appl. No. 09/885,959

Amdt. Dated: May 19, 2005

Reply to Office Action of: November 19, 2004

predetermined value and said components k_0 and k_1 are one half size of said scalar k .

7. (original) A method according to claim 3 wherein said value of said multiple kQ is calculated using simultaneous multiple addition.

8. (currently amended) A method according to claim 7 wherein ~~grouped terms G_i utilized in said simultaneous multiple addition are precomputed~~ includes precomputing a value G_i representing a grouping of like elements, said value G_i being used in said simultaneous multiple addition.

9. (currently amended) A method according to claim 6 wherein said components k_i are obtained by obtaining short basis vectors (u_0, u_1) of the field F , designating a vector v as $(k, 0)$, converting v from a standard, ~~orthonormal~~ orthonormal basis to the (u_0, u_1) basis, to obtain fractions f_0, f_1 representative of the vector v , applying said fractions to k to obtain a vector z , calculating an efficient equivalent v' in the composite representation of kQ .

10. (currently amended) A method of generating in an elliptic curve cryptosystem a key pair having a integer k providing a private key and a public key kQ , where Q is a point on the curve, the method comprising the steps of:

a) selecting an elliptic curve over a finite field F such that there exists an endomorphism ψ where $\psi(Q) = \lambda Q$ for all points $Q(x, y)$ on the elliptic curve, λ is an integer,

b) establishing a representation of said key k as a combination of components k_i and said integer

λ , of the form $k_i = \sum_{i=0}^{t-1} k_i \lambda^i \mod n$ where n is the number of points on the elliptic curve,

c) combining said representation and said point Q to form a composite representation of a multiple of the form ~~$k_0 Q + k_1 \psi(Q) + \dots$~~ $k_0 + k_1 \psi(Q) + \dots$ corresponding to the public key kQ ;

and

d) computing a value corresponding to said public kQ from said composite representation of kQ .

11. (previously presented) A method according to claim 10 wherein each of said components

Appl. No. 09/885,959

Amdt. Dated: May 19, 2005

Reply to Office Action of: November 19, 2004

k_i is shorter than said scalar k .

12. (previously presented) A method according to claim 11 wherein said components k_i are initially selected and subsequently combined to provide said scalar k .

13. (previously presented) A method according to claim 12 said components k_i are selected at random.

14. (previously presented) A method according to claim 13 wherein said representation is of the form $k_0 + k_1\lambda$.

15. (previously presented) A method according to claim 10 wherein said scalar k has a predetermined value and said components k_0 and k_1 are selected to be one half the size of said scalar k .

16. (previously presented) A method according to claim 12 wherein said value of said multiple kQ is calculated using simultaneous multiple addition.

17. (currently amended) A method according to claim 16 wherein ~~grouped terms G_i utilized in said simultaneous multiple addition are precomputed~~ includes precomputing a value G_i representing a grouping of like elements, said value G_i being used in said simultaneous multiple addition.

18. (currently amended) A method according to claim 15 wherein said components k_i are obtained by obtaining short basis vectors (u_0, u_i) of the field F , designating a vector v as $(k, 0)$, converting v from a standard, ~~orthonormal~~ orthonormal basis to the (u_0, u_i) basis, to obtain fractions f_i representative of the vector v , applying said fractions to k to obtain a vector z , calculating an efficient equivalent v' in the composite representation of kQ .